

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, LLC,
Plaintiff,

v.

Civil Action No. 2:21-CV-00137 (EWH)

PALO ALTO NETWORKS, INC.,
Defendant.

MEMORANDUM ORDER

This matter is before the Court on Palo Alto Networks, Inc.’s (“PAN”) Motion for Summary Judgment, ECF No. 460, and Motion to Exclude the Opinions and Testimony of Michael Mitzenmacher, Ph.D. (“Motion to Exclude”). ECF No. 495. The Court previously issued orders resolving the majority of issues raised in those motions, but reserved ruling on two issues: (1) PAN’s motion for summary judgment of no direct infringement of the ’380 Patent¹ and (2) PAN’s motion to exclude portions of Dr. Mitzenmacher’s opinion on the ’380 Patent as contrary to the Court’s claim construction order. *See* Mem. Order, ECF No. 690; Mem. Op. & Order, ECF No. 702. On January 4, 2024, the Court held a hearing to take up these issues.

For the reasons stated below, PAN’s motion for summary judgment of no direct infringement of the ’380 Patent is GRANTED. PAN’s motion to exclude portions of Dr. Mitzenmacher’s opinion on the ’380 Patent is DENIED AS MOOT.

I. LEGAL STANDARD

A. Summary Judgment

Under Federal Rule of Civil Procedure 56, a party may move for summary judgment on a claim or defense, or part of a claim or defense. Fed. R. Civ. P. 56(a). The district court will “grant

¹ U.S. Patent No. 10,735,380.

summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” *Id.* A fact is material if “its existence or non-existence would affect disposition of the case under applicable law.” *Wai Man Tom v. Hosp. Ventures LLC*, 980 F.3d 1027, 1037 (4th Cir. 2020) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). “A genuine question of material fact exists where, after reviewing the record as a whole, a court finds that a reasonable jury could return a verdict for the nonmoving party.” *Dulaney v. Packaging Corp. of Am.*, 673 F.3d 323, 330 (4th Cir. 2012) (citations omitted).

The movant bears the initial burden of demonstrating that there is no genuine issue of material fact. *Wai Man Tom*, 980 F.3d at 1037 (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986)). The nonmoving party must then establish that specific, material facts exist that would give rise to a genuine issue. *Id.* In reaching its decision, “the court must draw all reasonable inferences in favor of the nonmoving party, and it may not make credibility determinations or weigh the evidence.” *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000) (citations omitted).

B. Infringement

Infringement analysis is a two-step process: “[f]irst, the court determines the scope and meaning of the patent claims asserted, and then the properly construed claims are compared to the allegedly infringing device.” *Cordis Corp. v. Bos. Sci. Corp.*, 658 F.3d 1347, 1354 (Fed. Cir. 2011) (quoting *Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1454 (Fed. Cir. 1998) (en banc)). In order to show infringement, “the plaintiff must establish by a preponderance of the evidence that the accused device infringes one or more claims of the patent either literally or under the doctrine of equivalents.” *Bayer AG v. Elan Pharm. Rsch. Corp.*, 212 F.3d 1241, 1247 (Fed. Cir. 2000) (citations omitted). “To prove literal infringement, the patentee must show that the accused device

contains *each and every limitation* of the asserted claims.” *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1215 (Fed. Cir. 2014) (emphasis in original). “[I]f even one limitation is not met, there is no literal infringement.” *E.I. du Pont De Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1073 (Fed. Cir. 2019) (citations omitted). “Where a defendant seeks summary judgment of non-infringement, ‘nothing more is required than the filing of a . . . motion stating that the patentee had no evidence of infringement and pointing to the specific ways in which [the] accused [products] did not meet the claim limitations.’” *Novatek, Inc. v. Sollami Co.*, 559 F. App’x 1011, 1022 (Fed. Cir. 2014) (alterations in original) (quoting *Exigent Tech., Inc. v. Atrana Sols., Inc.*, 442 F.3d 1301, 1309 (Fed. Cir. 2006)). The burden of production then shifts to the patentee to “identify genuine issues that preclude summary judgment.” *Id.* (quoting *Optivus Tech., Inc. v. Ion Beam Applications S.A.*, 469 F.3d 978, 990 (Fed. Cir. 2006)).

II. DISCUSSION

Centripetal accuses three product combinations of infringing claims 16 and 25 of the ’380 Patent: PAN’s Next Generation Firewall (“NGFW”) with Advanced Threat Prevention (“ATP”); the NGFW with DNS Security Service; and the NGFW with Domain Fronting (collectively, the “’380 Accused Products”). Pl.’s Suppl. Objs. & Resp. to Def.’s 1st Set of Interrogs., App. A, ECF No. 462-33. PAN asserts that it is entitled to summary judgment because no reasonable juror could conclude that the ’380 Accused Products infringe—literally or under the doctrine of equivalents—either of the asserted claims of the ’380 Patent. Mem. in Supp. at 18–23, ECF No. 462. Specifically, PAN argues that Centripetal cannot establish that any of the ’380 Accused Products meet or perform the ’380 Patent claim limitation requiring that a packet security gateway “determine whether a value of the data transfer request field indicates that the data transfer protocol comprises one or more network exfiltration methods associated with [specified] packet

filtering rules” (the “determine element”). *Id.* at 19; *see* ’380 Patent at 13:57–14:2, 15:39–16:6.

Based on the undisputed evidence, the Court finds that PAN has met its initial burden under *Celotex* and that Centripetal fails to raise a genuine dispute of material fact that the ’380 Accused Products satisfy the determine element.

In relevant part, claims 16 and 25 of the ’380 Patent require a that a packet security gateway:

identify a data transfer request field within a header region of the identified at least one application packet;

determine whether a value of the identified data transfer request field indicates that the data transfer protocol comprises one or more network exfiltration methods associated with the one or more packet-filtering rules; and

apply one or more operators, specified by the one or more packet-filtering rules and based on a determination that the identified data transfer request field indicates one or more network exfiltration methods, to the first packets, wherein applying the one or more operators causes the first packets to be dropped.

’380 Patent at 13:57–14:2, 15:39–16:6.² In its claim construction order, the Court construed “header region of the identified at least one application packet” as the “application layer header of the identified at least one application packet.” Mem. Op. & Order at 15–19, ECF No. 452. Application-layer protocols, which are carried out at the application layer, include the Hypertext Transfer Protocol (“HTTP”) which may specify, in a data transfer request field, values such as GET, PUT, POST, and CONNECT. *Id.* at 18 (citing ’380 Patent at 7:13–16).

Accordingly, to show infringement, Centripetal must demonstrate that the ’380 Accused Products determine that a “value of the identified data transfer request field”—such as an HTTP GET, PUT, or POST value—“indicates that the data transfer protocol comprises one or more

² Both claims detail the same packet-filtering process. In claim 16 the process is performed by “one or more processors” and “memory comprising instructions” whereas in claim 25 it is performed by “non-transitory computer-readable media.” ’380 Patent at 13:36–41, 15:21–24.

network exfiltration methods.” Centripetal asserts that other packet information may also be considered in reaching this determination. *See* Resp. in Opp’n at 16, ECF No. 517 (“Nothing in the claim requires using only the application packet headers for this evaluation.”). PAN disputes this interpretation,³ but also argues that even if other packet information may be considered, Centripetal fails to present evidence that the ’380 Accused Products make any determination specific to the “identified data transfer request field.” Mem. in Supp. at 21–22, ECF No. 462.

Taking the evidence in the light most favorable to Centripetal, NGFWs pass application header information, which includes data transfer request field data (e.g., HTTP GET, PUT, or POST values), along with other information, to the machine learning model or advanced detection module. Mitzenmacher Opening Report, ’380 App. ¶¶ 89–93, ECF No. 517-3. For ATP and DNS Security services, this includes forwarding data to the cloud. *Id.* ¶¶ 7–8. The machine learning model or advanced detection module then returns a “verdict” to the NGFW indicating how it should proceed with processing the packet. *Id.* ¶¶ 122–134; *see also* Resp. in Opp’n at 16, ECF No. 517. At the motions hearing, PAN argued that the analysis that occurs in the cloud is not in evidence. Tr. at 68:8–15, 69:13–23, ECF No. 712. As a result, PAN asserts that Centripetal has not shown how the machine learning model or advanced detection module evaluates the data transfer request field (e.g., the HTTP GET, PUT, or POST values) and therefore has not shown that the ’380 Accused Products make a “determin[ation] whether a value of the identified data transfer request field indicates that the data transfer protocol comprises one or more exfiltration methods.” ’380 Patent at 13:59–63; Tr. at 68:8–15, 69:13–23, ECF No. 712.

³ The Court does not need to reach this first issue, in which the parties dispute whether other information may be considered at the determine step. Even assuming that Centripetal’s interpretation is correct, as explained below, Centripetal fails to establish a genuine dispute of material fact as to whether the determine element is satisfied.

Centripetal asserts that the evidence demonstrates “NGFWs use application header fields, such as HTTP header fields, to determine exfiltration.” Resp. in Opp’n at 16, ECF No. 517. More specifically, Centripetal maintains that the “NGFWs pass the application header information, which includes values of data transfer request fields, to one or more machine learning models or advanced detection modules which will render a verdict on whether the data transfer protocol . . . involves a data exfiltration attempt.” *Id.* Centripetal essentially argues that the allow/deny verdict made by the machine learning model or advance detection module is a determination as to whether the data transfer protocol involves a data exfiltration attempt. *Id.* However, all Centripetal can establish is that the data transfer request field value (along with other data) is sent to PAN’s machine learning models and advanced detection modules, that some unspecified analysis occurs, and thereafter a “verdict” is returned. This is not proof that “a value of the identified data transfer request field indicates that the data transfer protocol comprises one or more network exfiltration methods associated with the one or more packet-filtering rules.” ’308 Patent at 13:54–58. It is instead an invitation for unwarranted speculation. Centripetal’s evidence here is plainly insufficient to raise a genuine dispute of material fact.

In its opposition to summary judgment, Centripetal relies on the testimony of its infringement expert, Dr. Mitzenmacher. Dr. Mitzenmacher offers several different variations of his opinions which generally assert that the NGFWs “identify HTTP requests and response fields” and using “the context from the network traffic coupled with the data transfer protocol for outgoing data, the Accused Products determine whether the data transfer protocol comprises one or more network exfiltration methods.” Mitzenmacher Opening Report, ’380 App. ¶ 104, ECF No. 518-3. Dr. Mitzenmacher opines that because “NGFWs’ machine learning and advanced threat detection techniques use a variety of factors to detect network exfiltration,” the “process involves

determining if an HTTP request is used in network exfiltration.” Mitzenmacher Reply Report ¶ 77, ECF No. 518-2. Ultimately, Dr. Mitzenmacher opines that the Accused Products infringe the determine element in both claims of the ’380 Patent.

But Dr. Mitzenmacher’s opinions cannot stand alone without evidentiary support to create a material factual dispute. *Arthur A. Collins, Inc. v. N. Telecom Ltd.*, 216 F.3d 1042, 1047–48 (Fed. Cir. 2000) (“[T]he expert must set forth the factual foundation for his opinion . . . in sufficient detail for the court to determine whether that factual foundation would support a finding of infringement . . .”). And, as to this element, the factual foundation described by Dr. Mitzenmacher in his expert report is insufficient to create a genuine dispute of material fact. The evidence relied upon and characterized by Dr. Mitzenmacher indicates only that data transfer field values are sent to the machine learning model or advanced detection module, an unspecified analysis occurs, and a verdict is rendered. *See, e.g.*, Mitzenmacher Reply Report ¶ 77, ECF No. 518-2 (“PayloadTypeHTTPHeader is one data type analyzed by inline cloud.”); Mitzenmacher Opening Report, ’380 App., ¶ 104, ECF No. 518-3 (citing PAN documentation indicating the cloud “may require common data” or identify “all payload data”). This is also how Centripetal itself describes the technical documents it relies upon in its response to PAN’s motion for summary judgment. *See* Resp. in Opp’n at 15, ECF No. 517.⁴

As to each of the technologies that Centripetal asserts infringe in combination with the NGFW—ATP, DNS Security, and Domain Fronting—Dr. Mitzenmacher similarly opines that the infringing products satisfy the determine element but fails to support that assertion with any

⁴ Centripetal provides the Court with only two of the technical documents relied on by Dr. Mitzenmacher. *See* ECF Nos. 519-14, 519-15. The documents are cited only once in its brief and Centripetal provides minimal explanation, merely providing a parenthetical that one of the documents indicates “HTTP request header forwarded to cloud detection.” Resp. in Opp’n at 15, ECF No. 517.

evidence beyond the fact that the machine learning model or advance detection module receives and conducts some unspecified analysis on the information in the data transfer request field. Regarding ATP, Dr. Mitzenmacher opines that “NGFWs with ATP detect whether a data transfer protocol comprises one or more network exfiltration methods using the information in the packet as well as the context surrounding it.” Mitzenmacher Opening Report, ’380 App., ¶ 106, ECF No. 518-3. According to Dr. Mitzenmacher, “NFGWs forward packet and application layer header information to the cloud which uses machine learning to determine whether the HTTP request is likely for exfiltration.” *Id.* ¶ 107. However, his report provides no detail as to what the system uses the data transfer request field value for and whether, as part of its analysis, the system makes a determination that the *field value* indicates that the data transfer protocol comprises a network exfiltration method. Instead, Dr. Mitzenmacher’s report merely shows that these field values are among the information sent to ATP before it returns a verdict, and that they are analyzed in some fashion. The portions of the technical documents cited by Centripetal in its briefing are no different, merely demonstrating that that data transfer request field values are among the data sent to the machine learning model or advanced detection module. *See* Resp. in Opp’n at 15, ECF No. 517; ECF No. 519-14 at 237 (indicating that “[t]he cloud detection engines may require common data from [the] firewall,” including “http request header”); ECF No. 519-15 at 409 (indicating that “HTTP request” information is forwarded to the cloud).

Dr. Mitzenmacher’s opinions regarding DNS Security and Domain Fronting are equally lacking. While Dr. Mitzenmacher offers the opinion that DNS Security “can detect anomalies in the HTTP requests to malicious hosts that intend to exfiltrate data through DNS traffic,” he offers no detail on how this process occurs. Mitzenmacher Opening Report, ’380 App., ¶ 109, ECF No. 518-3. Further, the documents that Dr. Mitzenmacher relies on indicate that data transfer request

field values are only one type of information that DNS Security considers and fails to explain whether the system makes a determination that the *field value* indicates that the data transfer protocol comprises a network exfiltration method. *See id.* (“[O]ne item in DNS Security is to look at ‘Http POST/Put Sensitive information.’”). Similarly, Dr. Mitzenmacher’s opinion regarding Domain Fronting is largely conclusory and provides no description of how data transfer request field values are analyzed. *See id.* ¶ 110.

At the hearing on this matter, Centripetal’s counsel claimed that the Fed. R. Civ. P. 30(b)(6) deposition testimony of Nir Zuk and Jesse Ralston bridged this gap, providing an explanation of the innerworkings of PAN’s products prior to the exfiltration “verdict.” Tr. 104:22–105:5, ECF No. 712. However, the testimony only serves to underscore Centripetal’s evidentiary problem. Mr. Zuk was asked how PAN’s “Wildfire” technology detects command and control traffic. Videotaped Dep. of Nir Zuk at 73:14–76:25, ECF No. 518-13. Mr. Zuk explained that Wildfire sends known command and control traffic “into the machine-learning service,” and the “models can learn how to detect similar but not exactly the same command and control connections [in traffic passing through the NGFWs].” *Id.* at 74:11–20. He added that PAN’s products “extract information from the traffic, like HTTP data, data within HTTP, could be HTTP headers, it could be other things, depends on the situation, and we pass those through the machine-learning models to check whether its good or bad.” *Id.* at 75:25–76:5. While the Court can reasonably infer from this testimony that the machine-learning models may receive data transfer request field values, this evidence comes nowhere close to supporting a reasonable inference that PAN’s technology specifically “determines whether a value of the identified data transfer request field value indicates that the data transfer protocol comprises one or more network exfiltration methods.” ’380 Patent at 13:59–63.

The reference to Mr. Ralston's 30(b)(6) deposition testimony is even more perplexing. In its opposition brief, Centripetal does not cite Mr. Ralston's testimony in support of its "determine" element argument. And while Centripetal's counsel notes that Dr. Mitzenmacher relies "heavily" on Mr. Ralston's testimony in his expert report, Tr. at 105:3, ECF No. 712, the Court is not required to scour the record for unspecified evidence that might support Centripetal's argument. *Biotec Biologische Naturverpackungen GmbH & Co. KG v. Biocorp, Inc.*, 249 F.3d 1341, 1353 (Fed. Cir. 2001) ("It is not the trial judge's burden to search through lengthy technologic documents for possible evidence."). Nevertheless, having read the excerpts of Mr. Ralston's submitted as an exhibit to Centripetal's response in opposition to summary judgment, the Court can find no testimony that creates a genuine issue of material fact as to this issue. *See generally* Videotaped Dep. of Jesse Ralston, ECF No. 518-11.

Finally, Centripetal spent nearly the entirety of its time on this dispute at the hearing discussing an excerpt from an exhibit purportedly related to "use cases" for "Cobalt Strike" exfiltration attempts. *See* ECF No. 519-14 at 235. Specifically, counsel argued that language in the excerpt (stating, for example, "[n]eeded data: 1st HTTP GET request header – hold mode") meant that PAN's technology was using the "HTTP GET" data transfer request field value "to indicate a cobalt strike." Tr. 91:16–92:2, ECF No. 712. Centripetal chose to raise this highly technical argument for the first time at oral argument—it was not discussed *at all* in Centripetal's summary judgment briefing.⁵ This presents multiple problems. As an initial matter, under Rule 56(c), the Court cannot consider counsel's factual representations as evidence. *See Rountree v. Fairfax Cty. Sch. Bd.*, 933 F.2d 219, 223 (4th Cir. 1991) ("The arguments of counsel, absent any evidence such

⁵ Centripetal did cite to a separate page in the document with the parenthetical description: "HTTP request header forwarded to cloud detection." Resp in Opp'n at 15, ECF No. 517 (citing ECF No. 519-14 at 237).

as sworn affidavits accompanying objections to a motion for summary judgment, fail to meet the evidentiary standard necessary to create a genuine issue of material fact.” (citing *Celotex*, 477 U.S. at 324)). Additionally, raising this type of new argument at this stage implicates significant fairness concerns and, as such, the Court finds that it has been waived. *See Mulvey Construction, Inc. v. BITCO General Life Ins. Corp.*, No. 1:07-0634, 2015 WL 6394521, at *7 (S.D.W. Va. Oct. 22, 2015) (collecting cases explaining that a party waives an argument when it is raised for the first time at oral argument). But even considering the excerpt relied upon by Centripetal’s counsel does not change the analysis. From the face of the document alone, the Court can draw no reasonable inference related to the “determine” element. *See* ECF No. 519-14 at 235.

Further, Centripetal’s expert, Dr. Mitzenmacher, does not opine that this excerpt means what Centripetal’s counsel argues it means. Dr. Mitzenmacher references this excerpt three times: twice in the ‘380 Appendix to his opening expert report, and once in his reply report. Mitzenmacher Opening Report, ‘380 App. ¶¶ 73, 128, ECF No. 518-3; Mitzenmacher Reply Report ¶ 77, ECF No. 518-2. The two references to the excerpt in his opening report are not cited in support of the “determine” element. While Dr. Mitzenmacher does cite the excerpt in relation to the determine element in his reply report, the opinion suffers from the same problem as before—it does nothing to show the data transfer request field value was used to make an exfiltration determination. Specifically, Dr. Mitzenmacher references the excerpt in support of his statement that “[he] disagree[s] with the Villasenor Report that HTTP GET or POST were never analyzed to determine network exfiltration,” and explains in a parenthetical that the excerpt “show[s] ATP looks at HTTP request header and HTTP response header.” Mitzenmacher Reply Report ¶ 77, ECF No. 518-2. The problem is that evidence ATP “looks at” HTTP header data, which contains the data transfer request field, comes nowhere close to showing the data transfer

request field is used to determine exfiltration. These statements only lead to the reasonable inference that HTTP GET or POST were analyzed but do not shed any light on the purpose of the analysis. What is fatal is that there is no evidence of any determination specific to the data transfer request field and whether the values are indicative of network exfiltration methods. Accordingly, there appears to be no supporting evidence regarding counsel's explanation, and unsupported expert witness testimony cannot create a material dispute of fact that precludes summary judgment. *See DeLorme Publ'g Co., Inc. v. BriarTek IP, Inc.*, 60 F. Supp. 3d 652, 671 (E.D. Va. 2014) (citing *Krippelz v. Ford Motor Co.*, 667 F.3d 1261, 1269 (Fed. Cir. 2012)). Given this lack of evidence, Centripetal cannot establish that a genuine dispute of material fact exists as to whether the '380 Accused Products practice the determine element of the '380 Patent.

Dr. Mitzenmacher's doctrine of equivalents analysis largely repeats his literal infringement opinion and offers no additional evidence of how the '380 Accused Products meet the determine limitation. Dr. Mitzenmacher opines that the "['380] Accused Products perform this function in substantially the same way by using rules to analyze or determine the data transfer protocol based on information in the application header as well as data transfer request fields." Mitzenmacher Opening Report, '380 App. ¶ 119, ECF No. 518-3. This is no different from Centripetal's literal infringement argument that the determine step is satisfied because the evidence shows that, along with other information, the data transfer request field value is sent to the machine learning model or advance detection module, an unspecified analysis occurs, and a verdict is rendered. Resp. in Opp'n at 16, ECF No. 517. Centripetal offers no additional evidence in support of its doctrine of equivalents theory and such testimony alone is insufficient to establish infringement under the doctrine of equivalents. *See Lear Siegler, Inc. v. Sealy Mattress Co. of Mich., Inc.*, 873 F.2d 1422,

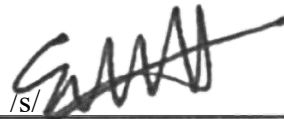
1425 (Fed. Cir. 1989) (“The evidence and argument on the doctrine of equivalents cannot merely be subsumed in plaintiff’s case of literal infringement.”).

Accordingly, the Court concludes that no reasonable juror could find that the ’380 Accused Products perform the determine element. PAN’s motion for summary judgment of no direct infringement of the ’380 Patent is granted. Because the Court grants PAN summary judgment of non-infringement of the ’380 Patent, it does not need to address PAN’s motion to exclude portions of Dr. Mitzenmacher’s testimony related to that patent.

III. CONCLUSION

For the reasons stated above, PAN’s motion for summary judgment of no direct infringement of the ’380 Patent, ECF No. 460, is GRANTED and PAN’s motion to exclude portions of Dr. Mitzenmacher’s opinion on the ’380 Patent, ECF No. 495, is DENIED AS MOOT.

It is SO ORDERED.

A handwritten signature in black ink, appearing to read "E. Hanes", is written over a horizontal line.

Elizabeth W. Hanes
United States District Judge

Norfolk, Virginia
Date: January 13, 2024